Questionnaire for
E-Gov Presidential Initiative or Line of Business
Standards Selection Process

Background:

Each E-Gov Presidential Initiative and Line of Business (LOB) requires the use of standards for deployment of innovative, web-based information technology (IT) services. Standards are required to ensure the necessary interoperability and security between government agencies, businesses, and citizens. Such standards are generally private sector, consensus-based standards. In cases where no suitable private sector standards are available, USG may develop and adopt government unique standards.

The Office of Management and Budget (OMB) has recognized the need to identify and validate appropriate and effective standards for E-Gov applications to ensure that the most effective standards are used in E-Gov applications and has assigned this responsibility to NIST. The lack of uniform, effective standards can lead to problems in internet accessibility, data compatibility, as well as national security and personal privacy concerns. NIST has established this E-Gov validation process to address such concerns and to assist federal agencies in the selection of appropriate E-Gov standards.

Instructions:

Please complete the questionnaire in its entirety and forward to:

Mary H. Saunders, Chief
Standards Services Division
100 Bureau Drive, MS 2100
Gaithersburg, MD 20899-2100

email: *mary.saunders@nist.gov*
fax: 301-975-4715

If you have any questions regarding the questionnaire you can contact David Alderman on 301-975-4019 (*david.alderman@nist.gov*) or Maureen Breitenberg on 301-975-4031 (*maureen.breitenberg@nist.gov*).

June 23, 2008

1. Title of E-Gov Initiative or Line of Business:
E-Authentication Initiative
The Office of Management and Budget (OMB) designated the General Services Administration (GSA) as the lead agency for the E-Authentication Initiative (Initiative), a cross-cutting initiative of the E-Government component of the President's Management Agenda. The Initiative was charged with developing a means of defining the levels of risk associated with online transactions performed between the public and government or between governments.

2. Initiative / LOB website:
http://www.cio.gov/eauthentication/index.cfm

3. Name and contact information for responsible Project Manager:
Tom Kireilis
Director, Strategic Solutions Division
Integrated Technology Services
Federal Acquisition Service
U.S. General Services Administration
Office: (703) 306-7698
Cell: (703) 589-2925

4. Name and contact information for questions regarding standards used in this initiative/LOB (if different from above):
SAME

5. Describe the process that was undertaken to choose and/or develop the standards required to implement the objectives of the Initiative or LOB:

With the approval of its Executive Steering Committee (ESC), a governance body comprised of representatives of the twenty-four (24) Chief Information Officer (CIO) Council agencies, the Initiative elected to pursue a federated approach to identity management to provide a standardized, government-wide means of authenticating End-Users of online government services, thereby reducing the risk to E-Government. The result was the creation of the Federation, a public-private partnership that enables citizens, businesses and government employees to access online government services using Credentials issued by trusted third-parties, both within and outside the government.

6. When determining standards needs were consensus standards given first consideration? If not, why?

Yes, The Authentication Service Component (ASC) provides the operational infrastructure of the Federation. The ASC is a recognized component of the Federal Enterprise Architecture (FEA) and, as such, is the recommended technical approach for online End- User authentication for Federal agencies.

7. Describe the process used to ensure that input from all appropriate stakeholders, public and private, was considered?
With the approval of its Executive Steering Committee (ESC), a governance body comprised of representatives of the twenty-four (24) Chief Information Officer (CIO) Council agencies

8. Please list participating federal agencies involved in selecting or developing and implementing standards for the initiative/LOB:

The E-Authentication Federation is managed by the E-Auth PMO in the Federal Acquisition Service of GSA. The Federation follows OMB M-04-04, which provides policy guidance for identity authentication, and National Institute for Standards and Technology (NIST) SP 800-63, which is the technical companion document to OMB M-04-04. The GSA Office of Government-wide Policy (OGP) provides policy support for the Federation.

9. Please list participating state or local governments agencies involved in developing and implementing standards for the initiative/LOB:
None

10. Please list participating private sector organizations involved in developing and implementing standards for the initiative/LOB:
Liberty Alliance

11. Please list participating voluntary consensus standards bodies involved in developing and implementing standards for the initiative/LOB:
Liberty Alliance

12. Please provide a list of standards relevant to the development and implementation of the initiative/LOB.

The ASC is a common infrastructure for electronically authenticating the identity of End-Users of E-Government services[3]. The ASC accomplishes this by leveraging Credentials from multiple CSPs through certifications, guidelines, standards adoption and policies – which is the basis of trust for Federation Credentials. In addition, the ASC supports varying levels of identity assurance (i.e., levels of confidence). Federation Members do not need to support every identity level of assurance. The ASC's broad range of authentication services to RPs makes separate credentialing unnecessary.

Currently, the ASC supports two architectural techniques for identity authentication within the same environment:

- **Assertion-based Authentication** – Personal Identification Number (PIN) and Password based authentication, where End-Users authenticate to a selected Credential Service (CS), which in turn asserts the End-User identity to the appropriate RP. An example of Assertion-based Authentication supported by the

ASC is *Security Assertion Markup Language (SAML) 1.0 Browser Artifact Profile.*

- **Certificate-based Authentication** – X.509v3 digital certificate based authentication in a public key infrastructure (PKI). Certification Authorities (CAs) issue certificates to End-Users, and End-Users present their certificates to applicable RPs for authentication.